Accellion Share Securely™

Accellion Security Overview

Ensuring Enterprise Data Security with Secure Mobile File Sharing.

Accellion, Inc.
1804 Embarcadero Road
Suite 200
Palo Alto, CA 94303

Tel +1 650 485-4300
Fax +1 650 485-4308
www.accellion.com
info@accellion.com

Security 0712

Overview

More than 1,500 Enterprise corporations and government agencies and 10 million enterprise users have chosen Accellion for securely sharing files and collaborating with colleagues, partners and vendors across organizational boundaries. Ensuring enterprise data security is a top priority for corporations and government agencies and is reflected throughout the Accellion secure mobile file sharing solution, in our processes, procedures and product design.

This document provides an overview of the Accellion security features designed to ensure protection of your enterprise data.

End to End Security

One of the best ways to understand the multiple levels of security of the Accellion secure mobile file sharing solution is to follow the path of a file from desktop, laptop, or mobile device through the Accellion system as users collaborate and share files. We have created a secure mobile file sharing system that allows organizations to protect their Enterprise content throughout the file sharing process.

Account Access and Authentication

Let's take a look at what happens when you start using Accellion for secure mobile file sharing. To get started, users have to log into an Accellion account.

Log-in Security Features

Robust and Flexible Password Policies

- Businesses can configure the password policies for their users:
- Password strength (number of characters, required number of numbers, special characters, restrictions from using email addresses)
- Password resets (a configurable time period)
- Password re-use restrictions
- Notifications after a configurable number of failed attempts
- Overall maximum session duration

Single Sign-on

Accellion offers Active Directory/multi-LDAP integration for Enterprise accounts. This gives Enterprise organizations centralized control and management over user accounts. Accellion supports single-on through SAML (Secure Assertion Markup Language) 2.0. SAML is an industry standard protocol for exchanging authentication and authorization information between different domains. Accellion supports multi-factor authentication through these single sign-on providers.

For information on Accellion single sign-on integrations, contact support@accellion.com.

File Sharing Security Features

After logging into the Accellion solution, users can quickly create secure workspaces, upload files, share files, add comments, subscribe to notifications and send files to stakeholders internal and external to the organization. Data is encrypted with 128-bit or 256-bit SSL encryption on transfer depending on the web browser. All files on an Accellion system are encrypted in transit and at rest.

Flexible and Robust Secure Workspace Permissions

Accellion enables you to control access to your Enterprise content across your organization.

File Tracking – Workspace managers can view activity logs to see who has accessed the workspace, downloaded, uploaded, and deleted files, and who has added comments, etc.

Notifications – Managers and contributors in a secure workspace can subscribe to notifications to receive emails when workspace members add files or make comments to files in their workspace.

Workspace – IT admins can set workspace and file expiration dates for their organization. Workspace managers can also set workspace and file expirations within the parameters set by IT.

Secure Links – Users can easily share files by sending stakeholders a secure link to a file in their Accellion Secure Workspace. Users can decide if the file can be downloaded by only the recipient of the email, if the recipient can forward the file to others, or if all authenticated users can download the file. They can set file link expiration dates. Users automatically get return receipts when files are downloaded.

Collaboration - Secure workspaces are designed to be shared with internal and external stakeholders. Workspace managers can manage users in their workspace and assign them with specified user roles depending on the business requirements.

Mobile Access Security Features

Mobile users can securely access their Accellion accounts through mobile browsers or the Accellion Mobile Apps for iPad, iPhone, Android and BlackBerry.

Accellion Mobile Apps support authentication through LDAP ensuring that only authorized users gain access to secure workspaces. Files saved on the mobile device are stored in a secure container with 256-bit AES encryption until they are opened using a supported editor application such as QuickOffice. Files shared with others via email are sent via the SSL protocol. Files downloaded to the device are password protected and encrypted while at rest. Users can choose a passphrase to access encrypted files downloaded to the mobile device using Accellion Mobile Apps.

With Accellion, IT admins can centrally manage and control mobile devices accessing corporate resources. IT admins can enable or disable mobile access for users. They can select Edit or View access for users depending on the security requirements of their organization. IT administrators have access to workspace activity logs ensuring data security and compliance. Accellion provides server based 256-bit AES encryption to enforce security policies from a central administrative dashboard. If a phone is lost or stolen, administrators can immediately disable access to Accellion. Admins can also disable accounts for mobile access if required and set expiration dates of files accessed through mobile devices.

In conjunction with MDM solutions such as MobileIron, BoxTone and Good IT can also ensure that only authorized apps are downloaded, users have the latest software updates, and users are not using excessive bandwidth. Lastly, if phones are lost or stolen, they can be remotely wiped to protect corporate data from getting into the wrong hands.

Storage

Files uploaded to your Accellion solution are stored either in the Accellion public cloud (Amazon EC2), or a private cloud (on premise using VMware, Citrix - XenServer, or Microsoft Hyper-V), or in a hybrid cloud depending on the deployment option you choose for your organization.

Public Cloud

Accellion provides single and multi-tenant storage in Amazon EC2 public cloud. Amazon security details are available in a later section of this document.

Private Cloud

Accellion supports private cloud on-premise deployment in VMware, Citrix XenServer, or Microsoft Hyper-V environments. Private clouds help organizations ensure the availability, integrity and confidentiality of their information. Located inside a company's firewall, private clouds are owned and controlled by IT allowing information to be solely managed by enterprises rather than delegated to third party cloud providers.

Encryption

Files are stored within the Accellion system on an encrypted partition using AES 128-bit encryption. Additionally, each file can be encrypted with a unique key. The file encryption key is also not stored on the server, so even if the server is compromised, the decryption keys for stored files cannot be obtained on the server itself. Data is also encrypted in transit using SSL/HTTPS.

Accellion's security mechanisms guard against malicious access:

- File names are de-referenced when stored on Accellion to ensure that files are inaccessible.
- Files may be stored encrypted for added security.
- Data can be accessed only through the file URL embedded in the email.
- Each URL call is authenticated individually.

Administrators do not have access to files once they are uploaded to the Accellion system. However, they can view the list of files and delete, replicate and set life cycle rules on these files. Administrators can also view reports and logs in relation to file access events.

Audit Trail

As an Enterprise-class mobile file sharing solution, Accellion automatically logs all file and user activities in the application. The audit log provides administrator's insight into what is being done in the system, which users are accessing files and, what files are being uploaded, and how the system is working overall. Audit trails and comprehensive file tracking help enterprise organizations demonstrate compliance with industry and government regulations. Audit logs are date/time stamped, and tracked by user, email address, IP address, and action taken. IT admins can sort by these attributes and also export the audit log either as a CSV file or to a Syslog server.

IT Admins set how long logs are stored on the Accellion system.

Global Settings

Accellion Mobile File Sharing is designed for enterprise organizations and is deployed and centrally managed by IT. IT administrators have the ability to centrally manage users across the globe through an Admin Console. They can set restrictions globally on user accounts, including:

- Who can create workspaces or upload files
- How long files are retained in the system
- Who can use Accellion Mobile Apps and whether users have View or Edit permission
- How many versions of a file are retained
- How long after files are deleted or expired can files be recovered
- Whether users can delete files

Data Retention

IT admins can set file and workspace life cycle rules and as well as select how long deleted and expired files are retained in the Accellion system. Organizations can have files stay in the trash from 1 to 180 days.

FIPS 140-2 Level 1

Accellion offers FIPS 140-2 Level 1 certified file sharing solutions for both on-premise and off-premise, virtual, cloud and hosted deployments.

Accellion Public Cloud – Amazon EC2

The Accellion Hosted Cloud Service extends Accellion mobile file sharing into the cloud. The service enables organizations to rapidly implement mobile file sharing to quickly scale resources and teams and manage peaks in usage. Accellion offers both single and multi-tenant public cloud deployment options through Amazon EC2

Reports and Certifications

Amazon Web Services (AWS) has completed multiple **SAS70 Type II** audits, and now publishes a Service Organization Controls 1 (SOC 1) report, published under both the **SSAE 16** and the **ISAE 3402** professional standards. AWS has also achieved **ISO 27001** certification, and has been successfully validated as a Level 1 service provider under the Payment Card Industry **(PCI)** Data Security Standard **(DSS).** *(Amazon, 2011)*

Physical Security

AWS datacenters are housed in nondescript facilities. Authorized staff must pass two-factor authentication a minimum of two times to access datacenter floors. *(Amazon, 2011)*

Data Privacy

AWS enables users to encrypt their personal or business data within the AWS cloud and publishes backup and redundancy procedures for services so that customers can gain greater understanding of how their data flows throughout AWS. *(Amazon, 2012)*

